1 FEMA Enterprise IT Architecture

1.1 Introduction

This section of the *FEMA IT Architecture* document provides the following:

- Discussion of background, scope, directives, organizations, missions, principles, operational environmental factors, and IT management team underlying and supporting the enterprise-wide *FEMA IT Architecture*
- Discussion of high-level FEMA business functions
- High-level information flow requirements and relationships
- Supporting applications and systems
- FEMA document and data descriptions
- Technology infrastructure (e.g., discussion of reusable IT architectural components).

Section 2 of this document provides the FEMA Technical Reference Model and Standards Profile. Section 3 discusses networking and communications aspects of the *FEMA IT Architecture*. Section 4 addresses maintenance and implementation of the *FEMA IT Architecture*.

1.2 Background of Enterprise Architecture

FEMA is a small Federal agency with a rather large information flow requirement to support widely-distributed planning and operations with FEMA's numerous business partners and the American public. Within FEMA, information technology, networking, and telecommunications resources are widely viewed as being **mission-critical** and **inseparable**.

FEMA has not had a formally defined, enterprise-wide, well-disciplined, and universally accepted information technology architecture (ITA) for development and integration of FEMA IT systems. However, with the establishment of the FEMA Switched Network (FSN) in 1982 and more recently with the development of the National Emergency Management Information System (NEMIS), FEMA has had a rather robust *implied* information technology architecture as a *de facto* agency-wide standard. The architectural standard is reflected in such enterprise-wide systems as NEMIS.

While this philosophical approach to architecture development has served FEMA well to date, the realization has come that it is now time for FEMA to formally define and document its information technology and network technology architectures. The goal is to achieve more efficiencies and higher levels of integration and interoperability, particularly with other Federal agencies, FEMA's partners, and the American public. This goal is congruent with the *Information Technology Management Reform Act (ITMRA)* as amplified by OMB Memorandum, M-97-16. With the passage of the ITMRA and the requirements of the OMB Memorandum, the FEMA Information Technology Services (ITS) Directorate views the development of a formal, enterprise-wide IT architecture as an important and timely opportunity to rigorously define and document the existing FEMA architecture. More important, the ITS Directorate and FEMA senior management also view this as an opportunity to manage FEMA's IT systems development in a more cost-effective, interoperable, scaleable, open, standardized, and secure manner in the future.

1.3 Directives for Development of the FEMA IT Architecture

The two major standards, policies, and guidelines that apply to this task include:

- ***Clinger-Cohen Act of 1996,* also known as the *Information Technology Management Reform Act.*** The ITMRA mandates policies and procedures for agencies to follow in the development and implementation of IT systems, including requirements for inter-agency coordination, technology transfer, performance, and business case analysis. The ITMRA formally established the position of the CIO within Federal agencies as the focal point for an agency's IT architecture development and management.

- **OMB Memorandum M-97-16, *Information Technology Architectures,* June 18, 1998.** This OMB Memorandum provides guidelines to Federal agencies on the development of their ITAs to meet the requirements of the ITMRA.

FEMA recognizes that decisions on IT architecture must be considered in the light of a number of other mandatory Executive directives, Congressional Acts, and judicial guidance documents. These documents are identified in Appendix I .

1.4 Scope and Definition of the FEMA Enterprise and the Enterprise IT Architecture

The *FEMA Enterprise* is simply and broadly defined to incorporate all internal and external resources (including partnerships) needed to accomplish FEMA's mission requirements. These resources include but are not limited to: personnel and organizations, Regional Offices and Disaster Field Offices (DFOs), IT resources and services, grant funds, corporate documents and data bases, partnerships with other Federal agencies with their commitments of resources, partnerships with state and local governments, FEMA facilities, fixed and transportable assets, partnerships and associations with voluntary organizations, security and Critical Infrastructure Protection (CIP) resources and measures, telecommunications and networking resources, other resources that can be impressed into service in the event of a national emergency, etc. Victims of disasters (and sensitivity to their concerns) are also considered an important part of the FEMA enterprise. Management of the FEMA enterprise clearly requires a robust FEMA enterprise information technology architecture.

The scope of this *FEMA IT Architecture* covers both information technology and network technology architectural components. This architecture does so in a seamless fashion because FEMA's mission-critical distributed information flow requirements demand (and frankly assume) a robust communications and networking backbone. The *FEMA IT Architecture* also broadly includes:

- Business processes
- Information flows (both internal and external)
- Automated and manual interfaces with FEMA partners and victims
- Hardware and software applications
- Documents and data stores
- Historical archives
- Accepted IT standards
- IT research and development resources

- Usable and reusable components of the National and Global Information Infrastructure (NII/GII)
- IT technology advances
- Other IT services and resources that can be impressed into service in a national emergency.

Consistent with OMB guidance, the *FEMA IT Architecture* provides the ***technology vision*** to guide resource decisions that will reduce costs and improve mission performance. The technology vision is considered within the scope of this initial *FEMA IT Architecture* document, but the detailed investment strategy and underlying cost-benefit analysis are not. The *FEMA IT Architecture* recognizes that technology and standards recommendations and improvements must be affordable. The *FEMA IT Architecture* sets the stage for cost-benefit analysis in an enterprise environment that is standardized and interoperable. A key presumption is that overall IT enterprise life-cycle costs will be reduced and mission performance will be enhanced through standardization activities. The ITA also sets the stage for FEMA to address Executive Order 13010 and Presidential Decision Directive 63 (PDD-63) concerned with Critical Infrastructure Protection (CIP).

For FEMA, one of the next steps is to prepare a comprehensive and tightly integrated IT investment strategy in accordance with OMB Memorandum M-97-02, dated October 25, 1996, entitled *Funding Information Systems Investments*. That memorandum states: *"Investments in major information systems proposed for funding in the President's budget should be consistent with Federal, agency, and bureau information architectures which: integrate agency work processes and information flows with technology to achieve the agency's strategic goals; and specify standards that enable information exchange and resource sharing."* This *FEMA IT Architecture* provides the required architectural input into the investment strategy process. FEMA is preparing to publish a separately prepared *Information Technology (IT) Capital Planning and Investment Guide.*

Consistent with PDD-63, FEMA is responsible for protecting its own critical infrastructure especially its cyber-based systems. The CIP directive presents significant IT architectural security challenges. The CIO for FEMA also serves as the Agency's Chief Infrastructure Assurance Officer (CIAO). By November 1998, the CIAO is responsible for proposing a plan for protecting FEMA's critical infrastructure, which shall include vulnerability assessments of IT and physical systems as well as recommendations for eliminating significant vulnerabilities. Response to the requirements of PDD-63 is a matter of high priority for FEMA.

1.5 Relationship of the FEMA ITA to Other High-Level Documents

FEMA is responsive to public laws, Executive Orders and other Presidential guidance, directives of other agencies (e.g., OMB, GSA, and NARA), court decisions, and FEMA's own rules and regulations as published in the *Federal Register* (such as the Code of Federal Regulations – particularly 44 CFR 1.1). These are listed in Appendices C and I.

From these national-level documents, FEMA has published FEMA enterprise-level documents that impact the *FEMA IT Architecture* including:

- *FEMA Strategic Plan*
- *Federal Response Plan (FRP)*
- *National Mitigation Strategy*

- *FEMA Annual Performance Plan*
- *Missions and Functions Manual 1010.1*
- *FEMA Information Resource Management Policy and Procedural Directive (FIRMPD)*
- *FEMA IT Capital Planning and Investment Guide*, draft.

1.6 FEMA's Mission and Principles

This section refines the scope and coverage of the ITA document and shows that the *FEMA IT Architecture* effectively bridges FEMA's high-level mission requirements with FEMA IT systems.

1.6.1 FEMA Mission Statement

The mission of FEMA is to **reduce the loss of life and property and protect our institutions from all hazards by leading and supporting the Nation in a comprehensive, risk-based emergency management program of mitigation, preparedness, response, and recovery.**

Mitigation	Mitigation is the process of taking sustained actions to reduce or eliminate long-term risk to people and property from hazards and their effects.
Preparedness	Provide the leadership, policy, financial and technical assistance, training, readiness, and exercise support to strengthen (1) community and Tribal readiness through preparedness and (2) the professional infrastructure of trained and tested emergency workers, community leaders, and public citizens who can prepare for disasters, mitigate against disasters, respond to a community's needs after a disaster, and launch an effective recovery effort.
Response	Response is the process of conducting emergency operations to save lives and property by positioning emergency equipment and supplies, evacuating potential victims, providing food, water, shelter, and medical care to those in need, and restoring critical public services.
Recovery	Recovery is the process of rebuilding communities so individuals, businesses, and governments can function on their own, return to normal life, and protect against future hazards.

1.6.2 FEMA Principles of Operation

This section briefly identifies and provides a consolidated listing of FEMA's principles of operation as they relate to design and integration of IT systems. From an IT architecture perspective, these principles provide a set of baseline requirements to be considered in the design, development, and integration of IT systems and networks.

- **Comprehensive Emergency Management (CEM).** The business functions above represent the phases of emergency management and comprise what public officials and emergency management professionals refer to as comprehensive emergency management (CEM). FEMA's organization, budget structure, strategic goals, and implementation strategies are

directly aligned in support of the Agency's mission and its core business functions. This *FEMA IT Architecture* establishes the baseline and target architecture for information technology and network technology to support the strategy of CEM. For FEMA, information technology represents a strategic resource and an important force multiplier to help support mission-critical business functions across the enterprise.

- **Mitigation as a cornerstone.** Within FEMA, mitigation is the cornerstone of CEM. Mitigation is an all hazards-based activity that is widely acknowledged to be information technology intense. Relative to IT systems, mitigation places a premium on intelligent collaboration and visualization along with the concept of creating, managing, using, and disseminating information. The volume of information is large and the demand for interaction with the information is growing rapidly.

- **Sensitivity to victims' concerns.** Sensitivity to the concerns of victims in a disaster is of paramount concern. The major implications for IT systems are that the systems be well-engineered and well-tested. In general, the public has zero tolerance for computer technology that does not work right, especially during time of a crisis.

- **Quality of Service.** Required Quality of Service (QoS) for IT systems and networks is an important design and integration requirement that needs to be addressed in a proactive manner. QoS should not be viewed with a "What you see is what you get" attitude, but rather as an opportunity for improvement. Perceptions of poor QoS need to be addressed and resolved.

- **Timeliness and responsiveness.** IT systems and networks must be designed to improve timeliness and responsiveness of service delivery; not impose delays or impediments to it.

- **Security.** IT systems and network security must be an integral part of the design and engineering process. Within the context of this *FEMA IT Architecture*, the term *security* encompasses document and data integrity, assured service availability, originator authentication, confidentiality, access controls, non-repudiation, and audit services. Security also encompasses the full scope of plans, policies, procedures, and measures necessary to achieve Continuity of Government (COG), Continuity of Operations (COOP), and Critical Infrastructure Protection (CIP). Requirements for an enterprise security architecture are addressed in Section 2.4

- **Results-oriented business sense.** The development of IT systems and networks needs to be results-oriented and to make business sense. The FEMA ITS Directorate desires to maximize the effectiveness of its investment portfolio in IT systems. FEMA will report on performance of both IT systems and the IT systems engineering process in accordance with ITMRA, GPRA, and customer service requirements.

- **Maximum leverage of IT, security, and telecommunications resources.** IT systems, security, and telecommunications are resources to be economized just like any other resource (e.g., funding, human resources).

- **Disciplined approach to IT systems development.** Emphasis needs to be placed on designing, developing, and integrating systems and networks in a disciplined manner across the FEMA enterprise. This includes establishment of accepted life-cycle models and enterprise-wide approaches for configuration management and systems engineering.

- **Standards.** To achieve interoperability and portability, IT systems and telecommunications standards are important and make good business sense. FEMA has a firm commitment to implement open systems approaches wherever practicable in coordination with its business partners.

- **Partnerships and coordination.** – In providing comprehensive emergency management, FEMA serves a vital coordination role toward achieving consensus across a significant number of external activities. IT systems and networks need to be designed, developed, and integrated in consideration of the systems for FEMA's business partners, the Regions, the States, and local governments. Consistent with PDD-63, close cooperation and coordination is also essential for a robust and flexible infrastructure protection program.

1.6.3 Overall FEMA Organization

Figure 1-1 depicts the FEMA organization. Each of the directorates is further divided into divisions and branches, which are discussed in more detail in the Business Function section of this *FEMA IT Architecture* document.

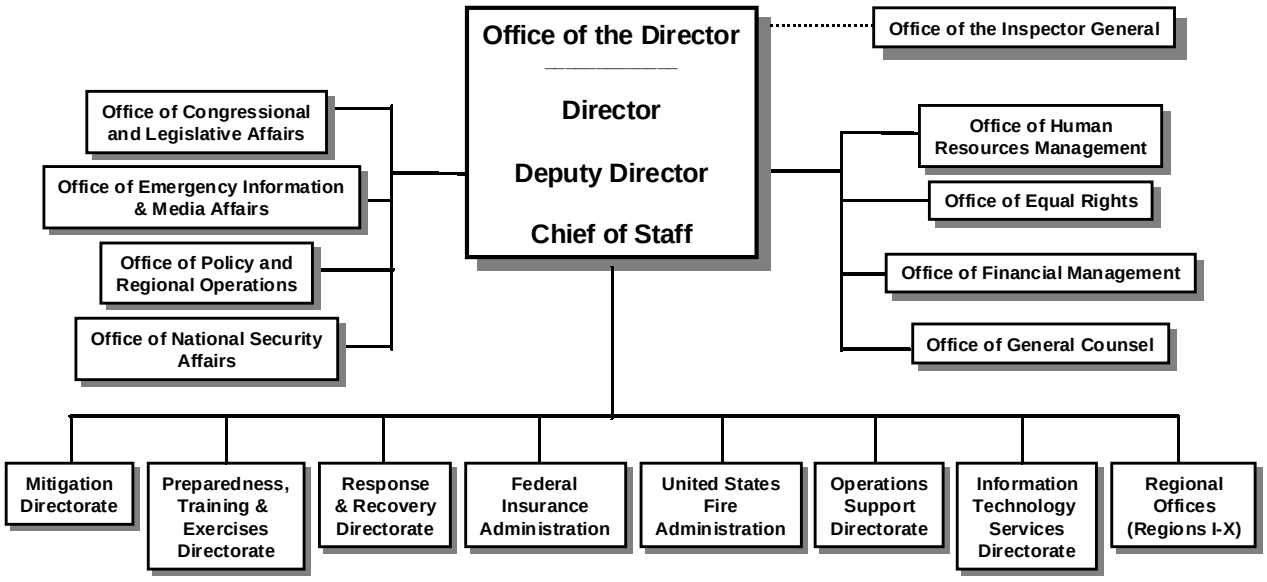

Figure 1-1. FEMA Organization at the Director, Directorate, Region, and Administration Levels

1.6.4 Missions and Responsibilities of Individual FEMA Organizational Entities

Table 1-1 identifies the major missions of the directorates and administrations identified in Figure 1-1. At the directorate and administration levels, FEMA organizational entities have a requirement for large and diverse information flows, both within FEMA and with external FEMA enterprise partners. Additionally, the information flow must generally be timely, accurate, and

precise. Also, the information exchange is often executed under emergency operational circumstances (see Section 1.6.6).

Table 1-1. Missions for FEMA Directorates and Administrations

Directorate or Administration	Mission Statement
Office of the Director	Provide leadership and direction to reduce the loss of life and property from all types of hazards through a comprehensive, risk-based, all-hazards emergency management program of mitigation, preparedness, response, and recovery.
Congressional and Legislative Affairs	Coordinate FEMA's ongoing emergency management dialogue with the U. S. Congress, and coordinate implementation of FEMA's legislative program.
Emergency Information and Media Affairs	Disseminate response and recovery information to the public and news media during and after natural disasters and other emergencies, inform and educate the public about emergency preparedness, and inform the public and constituent groups about FEMA's activities.
Policy and Regional Operations	Support the Director and Agency managers by conducting agency-wide planning; developing policy; implementing strategic initiatives; ensuring Regional coordination; and building partnerships with and among State and local governments, non-government organizations, business, and industry.
National Security Affairs	Serve as the focal point for FEMA activities related to terrorism, special programs, Continuity of Government (COG), Continuity of Operations (COOP), and Critical Infrastructure Protection (CIP). Ensure coordination of these activities within the Agency and with appropriate Executive Branch organizations through uniform and consistent national security policy in an all-hazards environment.
Inspector General	Serve as an independent and objective audit, investigative, and inspection unit relating to FEMA programs and operations for the purpose of promoting economy, effectiveness, and efficiency, or preventing and detecting fraud, waste, and abuse in FEMA programs and operations.
Human Resources Management	Plan and direct human resources programs to maintain a workforce capable of performing the Agency's assigned mission while advancing the Agency's commitment to its employees and the public.
Equal Rights	Serve the Agency and the nation by promoting affirmative employment, a discrimination-free workplace, and equal access to FEMA programs and benefits.
Financial Management	Promote sound financial management and accountability throughout the Agency by providing financial and acquisition-related guidance, information, and services to FEMA management and the Agency's customers.
General Counsel	As a staff element of FEMA, render legal advice and assistance on all matters related to Agency programs and operation.
Mitigation Directorate	Develop, coordinate, support, and implement policies, plans, and programs to eliminate or reduce the long-term risk to human life and property from natural and technological hazards, and support the Director in making mitigation the cornerstone of emergency management.

Directorate or Administration	Mission Statement
Preparedness, Training, and Exercises Directorate	Provide the leadership, policy, financial and technical assistance, training, readiness, and exercise support to strengthen (1) community and Tribal readiness through preparedness and (2) the professional infrastructure of trained and tested emergency workers, community leaders, and public citizens who can prepare for disasters, mitigate against disasters, respond to a community's needs after a disaster, and launch an effective recovery effort. Develop and implement customer service initiatives.
Response and Recovery Directorate	Develop and maintain an integrated operational capability to respond to and recover from the consequences of a disaster, regardless of its cause, in partnership with other Federal agencies, State and local governments, volunteer organizations, and the private sector. Maintain the deployable systems needed to support response activities such as the Mobile Emergency Response Support (MERS) Detachments. Manage the Urban Search and Rescue Task Force Program.
Federal Insurance Administration	Manage a Federal program to provide consumer-oriented flood insurance in participating communities.
United States Fire Administration	Provide leadership, coordination, and support for the nation's fire prevention, control, and emergency medical services (EMS) activities.
Operations Support Directorate	Provide logistics, security, health and safety, and other mission support services essential to the accomplishment of the Agency's all-hazards emergency management program.
Information Technology Services (ITS) Directorate	Provide agency-wide support for information technology services and systems for routine operations and in all-hazards emergency and disaster situations. Provide leadership and direction for management of information technology resources, automated data processing (ADP), telecommunications and information services, and systems necessary to support and accomplish FEMA's mission.
Regional Offices	Accomplish, within the Region, the national program objectives established for the Agency by the Director. Establish an all-hazards approach to emergency management throughout the Region through close working relationships with other Federal agencies, State and local governments, private industry, and local volunteer organizations in the implementation of FEMA policies and programs.

1.6.5 FEMA IT Management Team

The ITS Directorate is designated as the primary development authority and management authority for the *FEMA IT Architecture*. Lead responsibility is assigned to the ITS Management Division with the cooperation and assistance of the Program Management Group, the Operations Division, and the Engineering Division.

Under FEMA Instruction 1610.13, the ITS Directorate is tasked to provide technical, planning, and policy presentation support to the Information Resources Board (IRB).

FEMA Instruction 1610.13 defines the authority of the chairperson and designates the membership and responsibilities of the FEMA IRB. The FEMA Chief Information Officer (CIO) serves as the chairperson. The primary objectives of the IRB are to:

- Assist the CIO in the performance of FEMA's responsibilities under the ITMRA and the *Paperwork Reduction Act*

- Provide senior-level oversight of FEMA's information technology to promote the improvement of the Agency's practices in modernization, use, sharing, and performance measures

- Oversee development of FEMA's Strategic Plan that links information technology and associated funding

- Strengthen the management of information resources to ensure accountability

- Promote the management of information and information technology as strategic investments to pool resources, share experiences, and exchange ideas

- Identify opportunities for cross-cutting cooperation in using IT to support common functions and to integrate information technology on an agency-wide corporate basis.

The IRB provides advice to the Chairperson. The Chairperson makes the consensus and view of the Board known to the Director , and takes them into account in carrying out the CIO's responsibilities under the ITMRA and the *Paperwork Reduction Act*. IRB membership includes:

Principals
Chairperson, Chief Information Officer
Deputy Associate Directors, Deputy Administrators, and Office Directors for

- Mitigation Directorate
- Response and Recovery Directorate
- Preparedness, Training, and Exercises Directorate
- Operations Support Directorate
- Information Technology Services Directorate
- Federal Insurance Administration
- United States Fire Administration
- Office of Policy and Regional Operations
- Office of National Security Affairs
- Office of Financial Management
- Office of General Counsel
- Office of Emergency Information and Public Affairs (delegate)
- Office of Human Resources Management (delegate)
- Office of Inspector General (delegate).

Alternate
Senior staff member (Division level or above) as designated by the head of the organization

The IRB-sponsored Information Systems Policy Advisory Group (ISPAG) is responsible for:

- Developing and presenting recommendations

- Providing technical advice

- Identifying information resources issues that should be presented to the full Board

- Meeting with other information systems groups to enhance the subject matter knowledge of the IRB.

1.6.6 FEMA Operational Environment for IT Systems

With FEMA's mission to respond to disasters and emergencies that may be of national scope and significance and that may potentially threaten Continuity of Government (COG), FEMA IT systems and telecommunications resources must be designed, implemented, and integrated in due consideration of a full spectrum of contingencies that may arise. This is a critical architectural factor for development and implementation of FEMA ITA and network systems. The IT systems architects and engineers must know and understand the critical operational environmental factors and circumstances under which the system must operate.

This section briefly identifies the operational environmental factors that must be considered in the development of IT systems. It should be understood that not every FEMA business function is deemed as mission critical, nor does every FEMA business function require a robust and redundant IT support capability. On a day-to-day basis, most of FEMA's business functions are well handled in a normal business office environment. However, the potential always exists that FEMA will need to respond to contingencies that are extraordinarily severe. These contingencies place the most stringent of demands on mission-critical IT systems.

Major IT architectural implications for the following representative set of operational environmental factors are provided in Appendix J .

- Adverse weather conditions

- Local, State, and/or Regional infrastructure potentially destroyed or inoperable with a need to operate in a transportable environment

- Need for operations in a remote or rural environment (perhaps requiring a Disaster Field Office (DFO))

- Need for operations in a large destroyed urban environment (e.g., earthquake) – other than at FEMA HQ or a Regional Office

- Virtual/synthetic environment (for training, exercises, and simulations)

- Contingency operations and alternate facilities

- Office environment (e.g., FEMA HQ and Regional Offices including NFIP Regional Offices and Emmitsburg).

Many of the operational environmental factors often occur in combination. For example, adverse weather conditions such as a large hurricane can render infrastructure for an entire region inoperable and necessitate establishment of mobile and transportable support facilities.

1.7 FEMA IT Architectural Goals and Objectives

This section briefly identifies the major goals and objectives underlying the development of the *FEMA IT Architecture*. Consistent with the requirements of the ITMRA and OMB guidance, this *FEMA IT Architecture* documents the fundamental relationships among FEMA's business and management processes and information technology.

The major goals and objectives of the *FEMA IT Architecture* are to ensure:

1. Alignment of the requirements for FEMA's information systems with the processes that support FEMA's missions

2. Adequate interoperability, redundancy, and security of FEMA's information systems (consistent with the requirements for information assurance and critical infrastructure protection)

3. Application and maintenance of a collection of standards (including technical standards) by which FEMA will evaluate and acquire new systems and re-engineer existing systems.

1.8 FEMA IT Architectural Principles

This section and Appendix H of the *FEMA IT Architecture* establish the basic architectural principles upon which future FEMA IT systems will be designed, built, and acquired, and upon which legacy IT systems will be re-engineered. The architectural principles identified in Appendix H provide a stable foundation upon which FEMA developers, engineers, and integrators can make important IT systems design and implementation decisions. These principles are expected to evolve as FEMA's mission and business functions evolve. They will be periodically reviewed and their designation as FEMA IT architectural principles will be the responsibility of the CIO as advised by the FEMA IRB.

The FEMA CIO and IRB anticipate that an open systems, disciplined, and standards-based IT architecture will best meet FEMA's needs for designing and developing future information systems, for re-engineering legacy systems, and for achieving future integration and interoperability among systems across the broad and distributed FEMA enterprise. The open systems approach to IT systems across the FEMA enterprise is a fundamental architectural principle that must be employed. It follows that a closed-system, proprietary approach is strongly proscribed unless all reasonable avenues of opportunity for development of an open systems approach have been systematically eliminated and the approach has been agreed upon by the CIO in consultation with the IRB. Waivers and exceptions to the requirement to be open will be granted only under the most extraordinary of circumstances. Cost-benefit factors and operational exigencies may enter into this decision.

The architectural principles defined in Appendix H are mandatory for compliance. Except as indicated, the principles apply to new systems and any new development, interface, or integration of legacy systems. If a legacy system does not require re-hosting or new development, then these principles do not apply.

1.9 Snapshot of Current FEMA IT Architecture

In assessing and describing the status of the current FEMA IT and Network Technology Architecture (NTA), it is important to appreciate that the information and network architecture currently **is** meeting mission-critical operational requirements. However, many of the processes are manual and there is considerable ongoing effort to streamline and integrate systems. Figure 1-2 provides a snapshot or view of the architecture. Details of the current telecommunications and network architecture are provided in Section 3.

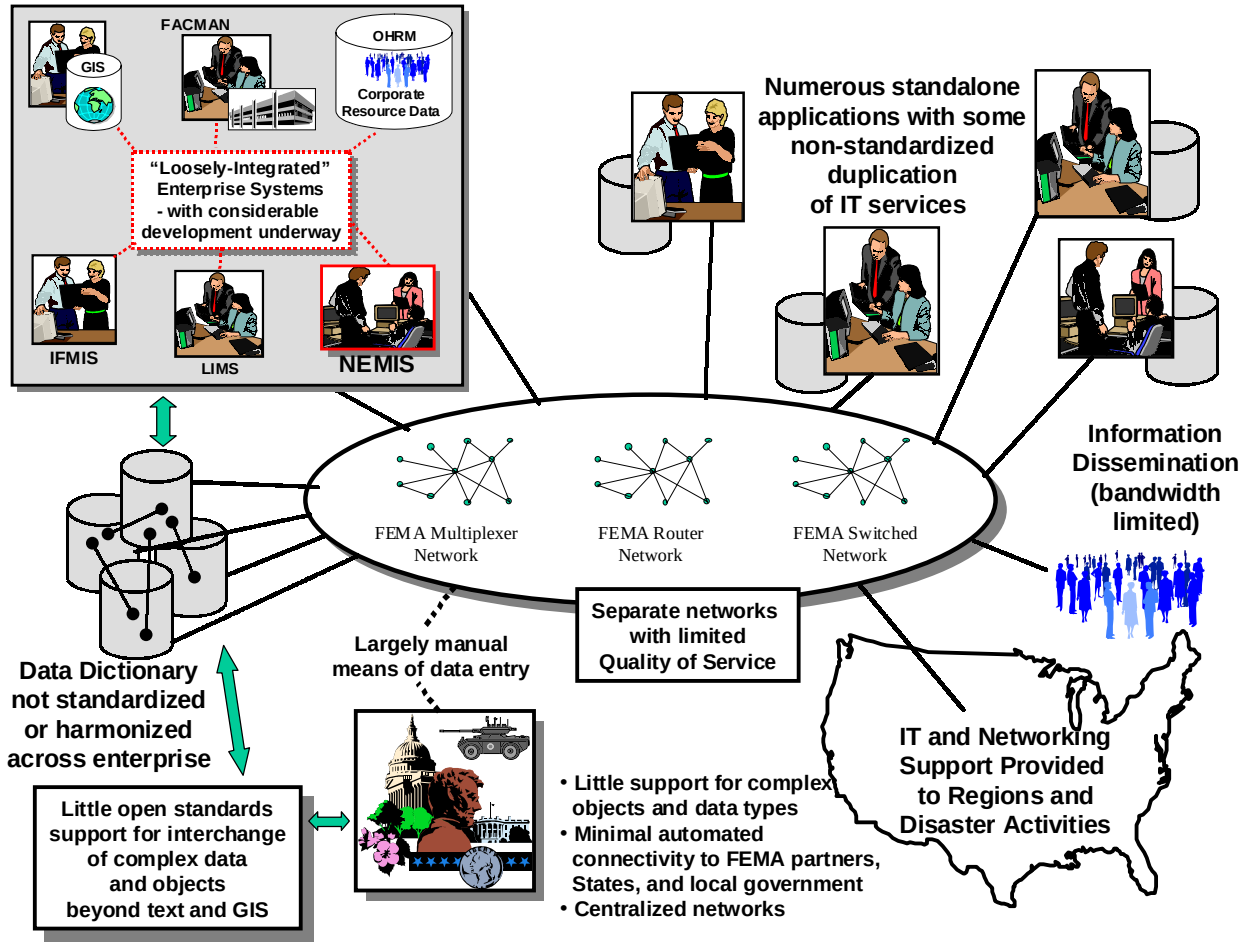

Figure 1-2. Snapshot of Current *FEMA IT Architecture*

From Figure 1-2, the following major characteristics of the architecture may be inferred:

- At the current time, FEMA is expending considerable effort to develop and integrate a number of enterprise-wide systems and activities including:
  - National Emergency Management Information System (NEMIS), which is operational in its Version 1 release
  - The Integrated Financial Management Information System (IFMIS)
  - The Logistics Information Management System (LIMS)
  - The Facilities Management (FACMAN) system
  - The FEMA Geographic Information System (GIS) with support from the Map Service Center (MSC) and the Map Analysis Center (MAC). An integrated capability is needed.

- Office of Human Resources Management (OHRM) corporate data bases supported by various information systems and servers

More detail on these systems is provided in Appendix M .

- Enterprise-wide systems are currently not as well integrated as desired. This largely reflects their current state of development. The ITS Directorate intends that the enterprise systems be better integrated in the target architecture environment.

- The FEMA Network Technology Architecture consists of separate sub-networks, including the FEMA Switched Network (FSN) and the FEMA Router Network/Multiplexer Network. Satellite communication and HF radio are also supported. Together, the networks meet minimal current operational requirements for voice, video (e.g., teleconferencing), and data. The network can be configured to provide limited Quality of Service (QoS) through manual reconfiguration of switches and multiplexers.

- FEMA has a basic problem resolution process and infrastructure to support FEMA networks, including a Help Desk and use of REMEDY to assist in tracking problems.

- FEMA has the capability to establish standalone communications in a disaster area where the communications infrastructure might be destroyed or out of order.

- The current FEMA network architecture is bandwidth-limited should the following IT applications be implemented:
  - Multimedia applications and graphics-intense interchange
  - Public information dissemination of multimedia objects such as streaming audio and video
  - Data-intense GIS applications (e.g., interactive GIS)
  - Intelligent distributed collaboration and visualization applications
  - Integrated voice, video, and data applications
  - Digital library applications where an enterprise-wide document management or text search capability might be incorporated
  - Virtual reality applications such as 3-D simulations for fire-fighting or telepresence.

- The current FEMA network architecture is largely centralized in its national operations and management (O&M). To date, security concerns have mostly limited establishment of Extranets, Virtual Private networks (VPNs), and gateways to FEMA enterprise partners and State/local governments (with coordination of the Regional Offices). Partly as a result, much of the data from external sources that is received in paper format must be manually scanned and/or re-keyed. The data that is received electronically from FEMA partners is mostly received as e-mail with attachments (most as word-processed documents).

- Configuration management of systems and networks is inconsistently performed and requires a standardized enterprise-wide solution.

- Data dictionaries for enterprise-wide systems and especially for standalone systems are not as well standardized and harmonized as desired.

- Numerous standalone systems (e.g., program-centric systems) in the various FEMA organizations have a need for common IT architectural components such as digital signature,